REMARKS

Applicant respectfully requests reconsideration of the rejection of this application as examined pursuant to the office action of February 13, 2006. In the office action, Claims 19-36 were examined. Claims 19-36 remain pending.

Claims 19-24, 26-28, and 30-36 were rejected under 35 USC § 103(a) as being unpatentable over Tibor (US Publication No. 2004/0234117) in view of Smith et al. (US Patent No. 6,918,038). Further in the office action, Claims 25 and 29 were rejected under 35 USC § 103(a) as being unpatentable over Tibor in view of Smith et al. and Ellingson (US Patent No. 6,871,287).

Applicant previously amended Claims 19, 22, 25-27, and 30 of the application to make it clear that the present invention is directed to a method and related system for protecting the identities of individuals. The method includes the steps of: a) establishing a database of known private information of one or more individuals, wherein the known private information includes one or more of personal information, financial information, criminal information, and authorized users and storage of such information; b) persistently scanning the Internet for stored private information of the one or more individuals stored in one or more other databases, wherein the persistently scanning occurs without requiring initiation through an action of the one or more individuals; c) replicating the stored private information of the one or more other databases gathered from the step of persistently scanning to a secure replication database; d) establishing indicia of unauthorized storage or use, or inaccuracies, of stored private information; e) recording location information of the one or more other databases containing the stored private information; f) comparing the known private information and the stored private information stored in the secure replication database; and g) notifying the one or more individuals when the indicia of unauthorized storage or use, or inaccuracies, of stored private information are detected. The system includes the features of: a) a first database of known private information of one or more individuals; b) means for persistently searching the Internet for one or more other databases containing stored private information of the one or more individuals, which means may be activated without initiation through an action by the one or more individuals; c) a secure replication database of the stored private information copied from the one or more other databases containing the stored private information; d) means for comparing the known private information of the first database with the stored private information of the secure replication database; and e) notification means for notifying any of the one or more individuals when the obtained stored private information for such individual or individuals differs from the known private information, is stored in one or more of the one or more other databases not authorized to have the stored private information, or a combination of the two.

The references cited in the February 13, 2006, office action, either singly or in any combination, fail to describe or teach the method and system of the present invention as claimed in the presently pending claims re-written above.

The primary reference cited in the office action is the published application of Tibor. Tibor describes an electronic transaction verification system, not a persistent private information protection system of the type described by the present invention. As stated in paragraph [0011] of Tibor:

> The present invention, in its simplest form, combines <u>the use of valid biometric samples</u> obtained from authentic identifications (IDs) with <u>biometric samples provided by a person at a transaction location</u>, thereby verifying that the biometric information presented for a transaction is a valid biometric for a particular person. In addition, the ID and the biometric sample can also be checked against known invalid users. Although it is possible for someone to counterfeit what is believed to be the authentic ID, in such cases, the identity thief provides an actual fingerprint that has been taken and placed on <u>the token or on the transaction slip</u>. When the token is returned to the transaction location as forged, counterfeit, stolen, etc., the fingerprint is entered into the database of known invalid users, thus preventing any further identity theft activity by this person on the verification system. The present invention, in its most complex form, adds additional safeguards, such as verifying the ID with information from the state. This ensures that an ID has not been altered, and is in fact an authentic state-issued ID (e.g., driver's license). Another such safeguard is verifying the information at the processing center of the token with the original information that a bank or token company obtained at the creation of the bank or token account. (Emphasis added.)

Tibor requires that a person: a) provide a biometric sample; b) present that sample at a transaction location; and c) submit a token or a transaction slip in association with an intended transaction. The Tibor system then transmits the obtained biometric sample, such as a fingerprint, to a database for comparison to a known digitized version of the biometric sample. If there is a match, the transaction is approved and may proceed. If there is no match, the transaction may be denied, and the occurrence may be cataloged. Tibor simply provides a mechanism for protection, primarily, of a merchant by improving the opportunity to deny transfer of money, goods, etc., to an unauthorized individual. On the other hand, the present invention is designed primarily to protect the individual and, indirectly, those who lawfully retain the individual's private information in their databases. The present invention does not require a transaction event initiated by the individual to trigger a biometric sample matching event. Instead, the present invention scans for inaccurate private information or misused private information and acts upon detecting such inaccuracy or misuse.

Applicant also notes that the published application of Tibor was filed on April 1, 2004, as a continuation-in-part of the application serial no. 09/335,649, filed June 18, 1999, now US Patent No. 6,728,397 (the '397 patent). Applicant's representative has reviewed the published application and compared the text thereof with the text of the '397 patent. Firstly, it is to be noted that the '397 patent was clearly directed solely to the concept of verifying a negotiable instrument, a check more particularly, offered at a point of sale. Secondly, many of the sections of the Tibor published application cited in paragraph 3 of the April 26, 2005, office action were modified from their corresponding sections of the '397 patent. For example, paragraph [0011] of the Tibor reference was not in the '397 patent. Paragraph [0012] of the Tibor reference, corresponding to column 1, line 64, to column 2, line 14, of the '397 patent, includes additional and expanded descriptions of the information scanned from the negotiable instrument and data transfer. Paragraph [0030] of the Tibor reference, corresponding to column 3, line 65 to column 4, line 20, of the '397 patent, includes additional and expanded descriptions of the "identification database." Paragraph [0034] of the Tibor reference, corresponding to column 5, lines 25-37, of the '397 patent, includes additional and expanded descriptions of the processing of data and the information contained in the database. The '397 patent makes no mention in that section of the patent to a plurality of databases as described in paragraph [0035] of the Tibor reference.

In addition to the substantial differences between the published Tibor application cited and the '397 patent containing lesser information, Applicant respectfully suggests that the reference fails to teach one or more of the components that the February 13, 2006, office action indicates are taught. Specifically, on the one hand it is stated in paragraph 3 of the office action that Tibor does not explicitly teach "persistently scanning one or more network communication systems for stored private information … requiring initiation through an action of one or more individuals; replicating the stored private information, while on the other hand, in that same paragraph, it is stated that Tibor teaches "persistently scanning one or more network communication systems for indicia (see paragraph [0030] and [0035]) ..." However, a review of the noted sections of the Tibor reference makes clear that Tibor provides no such teaching. Paragraph [0030] of the Tibor reference states:

> Referring now in greater detail to the drawings, in which like numerals represent like components throughout the several views, FIG. 1 illustrates a block diagram of an exemplary embodiment of the verification system illustrating an electronic transaction verification unit 10 in communication with a central processing system 12 that includes·an identification database 14. The identification database can include a number of databases used in the identification process such as a biometric database of known customer data, as well as a separate database of known invalid users. The database of known invalid users can be established by correlating a biometric presented at a transaction location that is used with a fraudulently obtained transaction token, and storing the biometric as invalid. Central processing system 12 can be a main system remote from the transaction location. While a check is disclosed as one type of token to be processed in an exemplary embodiment of the present inventive system, other tokens can be processed in the same manner as disclosed herein. Negotiable instrument, as the term is used herein is defined in Article 3 .sctn.104 of the Uniform Commercial Code. An instrument is negotiable if it is: (1) a written instrument signed by the endorser or maker; (2) an unconditional promise to pay a certain amount of money, either on demand or at a future date; and (3) payable to the holder or bearer. Examples of negotiable instruments are checks, bills of exchange, and promissory notes. A check as used herein means a draft, payable on demand and drawn on a bank, or a cashier or teller's check. This is the customary definition of a check. The exemplary embodiment of the electronic transaction verification unit 10 is comprised of, at least, a check scanner or token reader 16 and a biometric data-gathering device 18, such as a fingerprint recording device.

Nowhere in paragraph [0030] of the Tibor reference is there any mention of "persistently scanning" (Claim 19 of the present application) or "persistently searching" (Claim 26 of the present application) one or more databases that may contain private information for the purpose of relating that information with known private information. Paragraph [0030] further makes clear that Tibor only reviews its own known customer data or a database of invalid users when initiated by a transaction occurring through an action of an individual, namely, the attempt to conduct some form of funds transaction. Tibor would not detect an error in private information contained in a database, including a legitimate database. Tibor would not move to detect, for example, the storage of an individual's credit card information stored in an unauthorized database unless and until a transaction was initiated. The present invention, on the other hand, persistently checks databases for the individual's private information and, if determined to have defined indicia, such as unauthorized storage of the credit card number, the individual would be notified before an unauthorized transaction is initiated that such unauthorized storage exists. Preventive action may then be undertaken, rather than corrective action.

Similarly, paragraph [0035] of the Tibor reference fails to describe the persistent scanning or searching. Paragraph [0035] states:

> At the central database 30, the incoming data is compared, either in parallel with or separately with token identification data, with the existing known data for authorized users of accounts, shown by decision block 32, and an approval is made as to whether or not to accept the token. Either a yes decision 34 or a no decision 36 on approval is then re-transmitted back to the computer hardware platform 28 of the check verification unit 10. While the check verification unit 10 is shown in communication with a database 30 remotely located thereto, it is not necessary that the central system 12 or the database 30 be located remotely to the electronic transaction verification unit 10. In fact, the electronic transaction verification unit 10 and central system 12 can be self-contained at the transaction location whereby the central database, or the account information and biometric databases are continually updated within the electronic transaction verification unit 10 through either a data connection to a master database or through periodic manual updates from storage media such as floppy disks or CD ROMs. In such an embodiment, the electronic transaction verification system is preferably self-contained and includes all the necessary devices for scanning drivers' licenses 20, gathering biometric data (e.g., fingerprints) 18, or scanning checks/reading tokens 16 (gathering check or token information data) within one unit comprising the system.

Nowhere in paragraph [0035] of the Tibor reference is there any mention of "persistently scanning" (Claim 19 of the present application) or "persistently searching" (Claim 26 of the present application) one or more databases that may contain private information for the purpose of relating that information with known private information. Paragraph [0035] makes reference to "continually updated," but that is only in respect to the relationship between the central database or account and biometric databases, and the master database. Nowhere in paragraph [0035] is it suggested that any database not under direct control of the system is persistently scanned or searched for the individual's private information. Instead, it is likely that updating in respect of a particular individual's information is only triggered as a result of a transaction. The present invention, on the other hand, persistently checks databases, including ones not under the system's direct control, for the individual's private information. Upon determination that detected information varies with known information, the individual is notified, the error corrected, or a combination of the two.

While not previously cited in other office actions for the present application, the February 13, 2006, office action cites as relevant to the present invention the apparent teachings of the Smith reference. In particular, Smith has been cited as teaching "persistently scanning the Internet for stored private information … requiring initiation through an action of the one or more individuals; replicating the stored information …" The examiner cites column 4, lines 43-63, and column 17, lines 36-66, for support of this assertion.

Applicant respectfully disagrees that Smith in any way teaches these features of the method and system of the present invention as described in the pending claims. Smith is directed to a system for protecting software distribution. See column 1, lines 17-23. Smith also indicates that the technology is directed to protecting distributed and stored data from theft. See column 3, lines 1-4. Nowhere does Smith suggest that the technology is directed to detecting unauthorized usage of information stored on any type of database other than private network controlled by the system described by Smith. The present invention is as different from the technology of Smith as it is different from the technology of Tibor.

It is important to incorporate into this response the sections of the Smith reference cited in the office action to show why Applicant submits that the Smith reference is inapplicable. Firstly, Column 4, lines 43-63, of Smith states:

> Where data security is a concern and the protection of data is necessary, the present invention includes mechanisms to prevent unauthorized copying or alteration of electronically stored and transmitted data by outsiders (e.g., "pirates") and trusted insiders. For example, the system performs generation and subsequent operation of a secure network without revealing embedded detailed security measures to software developers. The network includes a plurality of linked nodes, wherein each node is formed from the installation of a software application on a predetermined remote computer or target site. A monitoring capability is used to ensure security is maintained and to respond to security violations and human auditing of the network may be employed to verify proper installation in accordance with a network definition template. Once completed, the template substantially defines, in human readable form, the network from a top level, including identification of each node, identification of each link between nodes, identification of data types to be exchanged between nodes, and identification of a software application to be installed as part of each node. A set of agent library functions is included with the application to facilitate communication of each node with the rest of the network.

The examiner contends that this passage describes either or both of persistently scanning the Internet for stored private information requiring initiation through one or more individuals, and replicating the stored private information. A clear reading of that passage yields no support for that interpretation. The limitation of the presently pending claims related to the first aspect of this apparent Smith teaching is "persistently scanning the Internet for stored private information of the one or more individuals stored in one or more other databases, wherein the persistently scanning occurs without requiring initiation through an action of the one or more individuals". The noted passage of Smith makes no mention of scanning the Internet. It is directed solely to protecting a private network from unauthorized probes for information. Further, nowhere in the quoted passage does Smith suggest that the scanning is performed with respect to any particular individual without any initiation by that individual. The monitoring apparently described by Smith checks for internal or external attacks of its own network. That passage further describes means for identifying nodes of the secured network. The present invention is not directed to network security of the type described by Smith. Instead, it is directed to the protection of the information of private individuals.

In addition, the noted passage fails to make any reference to the other limitation of the claims of the present invention the examiner contends is taught. Specifically, the present invention includes "replicating the stored private information of the one or more other databases gathered from the step of persistently scanning to a secure replication database." Nowhere in that passage does Smith suggest replicating stored information of the individual to a secure replication database. Further, Smith fails to teach that such a secure replication database is used to deny unauthorized users from learning that an individual is seeking information about the unauthorized usage of his/her information. As noted, Smith is simply not directed to such an identity protection method and system. Smith is only directed to software protection and private network security.

The remaining passage of Smith cited in the office action is at column 17, lines 36-66. That passage states:

> A monitor node **674** (or "monitor") manages the security of the network, the strobing of keys and passwords, and the termination of a node or the network in response to a security violation. Because of its unique interaction with the other nodes in the network, monitor node **674** must be the first node installed. Monitor node **674** links to each other network node as the nodes are installed and there is a unique key pair for each of those links. Like other nodes, monitor node **674** has a

> private and public key pair used for encrypting data sent to other nodes. The monitor node may be installed on the installation server **630** or on an independent computer and linked into the network. It is recommended that the monitor be maintained in a highly secure environment, preferably inside a secure room, and preferably on a machine on which the monitor is the only application. In other embodiments, there may be more than one monitor node per network, particularly if the network is segmented into subnetworks. In such a case, a subnetwork may have its own monitor node.
> A particular example of a network **600′** with more than one monitor node is shown in FIG. 6B. In FIG. 6B, network **600′** is shown with two monitor nodes, **674** and **676**, located on separate secure machines **670** and **675**. In this configuration, nodes **646, 656,** and **666** will be monitored by monitor nodes **674** and **676**. The connections between monitor node **674** and nodes **646, 656,** and **676** are installed by agent modules **642, 652** and **662**, respectively, which are generated by generator **620**. The connections between monitor node **676** and nodes **646, 656,** and **676** are installed by agent modules **648, 658** and **668,** respectively, which are generated by generator **622**.

This passage of Smith is directed to the details of maintaining the security of a private network, which is consistent with the focus of the technology described throughout the Smith reference. More particularly, the examiner contends that this passage describes either or both of persistently scanning the Internet for stored private information requiring initiation through one or more individuals, and replicating the stored private information. A clear reading of that passage yields no support for that interpretation. The limitation of the presently pending claims related to the first aspect of this apparent Smith teaching is "persistently scanning the Internet for stored private information of the one or more individuals stored in one or more other databases, wherein the persistently scanning occurs without requiring initiation through an action of the one or more individuals". The noted passage of Smith makes no mention of scanning the Internet. It is directed solely to protecting a private network from unauthorized activity, such as seeking access to information. Further, nowhere in the quoted passage does Smith suggest that the scanning is performed with respect to any particular individual without any initiation by that individual. The present invention is not directed to network security of the type described by Smith. Instead, it is directed to the protection of the information of private individuals.

In addition, the noted passage fails to make any reference to the other limitation of the claims of the present invention the examiner contends is taught. Specifically, the present invention includes "replicating the stored private information of the one or more other databases gathered from the step of persistently scanning to a secure replication database." Nowhere in that passage does Smith suggest replicating stored information of the individual to a secure replication database. Further, Smith fails to teach that such a secure replication database is used to deny unauthorized users from learning that an individual is seeking information about the unauthorized usage of his/her information. As noted, Smith is simply not directed to such an identity protection method and system. Smith is only directed to software protection and private network security.

The examiner contends in the February 13, 2006, office action that "It would have been obvious at the time the invention for one of ordinary skill in the art to have combined the teachings of Tibor and Smith" to teach the persistent scanning and replication steps of the present invention. It may be that Tibor and Smith are compatible technologies, but nowhere is it taught or suggested in either reference to look to the other to create a system as described and claimed in the presently pending application. Neither is directed to searching out for unauthorized usage of individuals' information and pulling that information into a secure replication database. These references simply do not teach any such features. They do not do so singly or in combination. They do not teach to look to the other to describe the present invention.

In view of the current limitations of independent Claims 19 and 26, and the arguments presented herein regarding Tibor and Smith, Applicant respectfully suggests that the 35 USC § 103(a) rejection of Claims 19-24, 26-28, and 30-36 has been successfully traversed. Withdrawal of that rejection is therefore requested.

Claims 25 and 29 were rejected under 35 USC § 103(a) as being unpatentable over Tibor in view of Smith and Ellingson. Applicant incorporates herein by reference the statements presented above with regard to the Tibor and Smith references. Applicant further notes that Ellingson fails to teach the present invention as claimed, whether or not combined with either or both of Tibor and Smith. Ellingson provides no indication of a system for persistently scanning or searching databases for private information as it relates to known private information, and doing such scanning or searching without first requiring a triggering action by the individual who is the subject of the searching. Ellingson appears to be relied upon as teaching the concept of different types of databases and the replication thereof, as well as search engine types. The present invention as claimed in the noted claims is directed to an identity theft protection system employing such search engines. The database types are not claimed alone. The search engine types are not claimed alone. Moreover, neither Tibor nor Smith teaches or fairly suggests relying upon Ellingson to teach such scanning or searching steps or arrangements.

In view of the current limitations of independent Claims 19 and 26, and the arguments presented herein regarding Tibor, Smith and Ellingson, Applicant respectfully suggests that the 35 USC § 103(a) rejection of dependent Claims 25 and 29 has been successfully traversed. Withdrawal of that rejection is therefore requested.

CONCLUSION

In view of the current state of claims and the arguments presented herein, Applicant respectfully suggests that the presently pending claims clearly describe the present invention and distinguish it over the cited Tibor, Smith and Ellingson references. It is therefore requested that this application be allowed to pass to issuance.

Applicant notes that no new claims have been added by this amendment. Therefore, no additional filing fee is required.

Respectfully submitted,

Chris A. Caseiro, Reg. No. 34,304
Attorney for Applicant
Verrill Dana, LLP
One Portland Square
Portland, ME 04112-0586
Tel. No. 207-253-4530

Atty Docket No. PAGE-001

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the US Postal Service in an envelope with sufficient postage as first class mail and addressed to Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on March 24, 2006. It is hereby requested that this communication be assigned a filing date of March 24, 2006.

Chris A. Caseiro